METHOD AND APPARATUS FOR DEFENDING AGAINST DENIAL OF SERVICE ATTACKS WHICH EMPLOY IP SOURCE ADDRESS SPOOFING

Field of the Invention

The present invention relates generally to the field of Internet security and more particularly to the problem of defending against denial of service (DoS) attacks which employ IP (Internet Protocol) address spoofing.

Background of the Invention

In today's Internet, when a packet is delivered from a carrier to a customer, there is no accurate information about where it came from. The source IP address in the packet header can be (and in denial of service attacks, frequently is) forged. There have been several attempts in the past at solving this problem.

One prior art solution is for the customer (perhaps as a managed service) to install IPsec VPN (Virtual Private Network) hardware, familiar to those of ordinary skill in the art, effectively creating a point-to-point path across the Internet by means of encryption. This is secure, although effort must still be expended to discover and discard malicious packets.

A second prior art solution is the use of the BGP (Border Gateway Protocol) VPN, in which customer-specific virtual routers are used to segregate traffic. This can also work, though complexity is generally regarded as the enemy of security and the substantial extensions to BGP involved are anything but simple.

A third prior art solution is for the carrier to provide perfect ingress filtering, as is well known and described, for example, in IETF (Internet Engineering Task Force) RFC (Request for Comments) 2267. In practice, what this would mean is that the carrier would have a set of addresses for its customers spanning a certain range. At each customer connection, only packets with source addresses belonging to that customer would be allowed to enter. At peering connections to the rest of the Internet, any incoming packets with source addresses in the carrier's range would be dropped. In this way, a customer could depend on the source address of a packet that it receives, as long as the address is in the correct range.

There are sometimes legitimate uses for forged packets, however, so a dogmatic implementation of ingress filtering will lead to problems, though probably fewer than are already caused by Network Address Translation. The much more difficult problem is that universal deployment by carriers worldwide is very far off, if it is even possible (logistically). Some of the reasons that ingress filtering is not popular include (i) it provides no revenue stream to the carrier; (ii) carriers are concerned about asymmetric routing; and (iii) it is ineffective unless it is very widely deployed.

Summary of the Invention

The present invention provides a novel solution to the above-described problem – one which can advantageously be incrementally deployed. In accordance with certain illustrative embodiments of the present invention, a carrier offers a

"premium" service which comprises marking packets for which it has in fact been able to verify the source address. According to one such embodiment, this marking flag is implemented by setting the Type-of-Service (TOS) field in the IP header to a non-zero value if and only if the source address of the packet has been verified. Note that, as used herein, the terms "marking" and "setting" of a "flag" or a data "field" merely signify the act of "ensuring" that the given flag or data field does in fact contain the desired value (*e.g.*, zero or non-zero), regardless of whether the desired value is actively written to the flag or data field or whether the current value of the flag or data field is first checked and then overwritten only if the current value is *not* the desired value. Also note that we will refer to such a (premium) service herein as "IP CallerID" because it accurately identifies (*i.e.*, verifies) the source address of an IP packet in a similar sense to that of conventional telephony CallerID which identifies the source address (*i.e.*, telephone number) of a telephone call.

For example, in accordance with one illustrative embodiment of the present invention, any packets entering the carrier's network from customer access links that fail to pass a Reverse Path Forwarding (RPF) or other test would advantageously have the TOS field thereof set to a zero value, while packets which do pass such a test would advantageously have the TOS field thereof set to a non-zero value. (As is fully familiar to those of ordinary skill in the art, a Reverse Path Forwarding test comprises checking at a network ingress port that an incoming packet having a given identified source address is, in fact, being received on the same port that it would have been routed out to, if it were instead an outgoing packet having a destination address equal

to its identified source address.) Also, in accordance with one illustrative embodiment of the present invention, a non-zero value (*e.g.*, a value of one) is written to the TOS field if it has passed the RPF (or other) test *only if* the TOS field has not already been set to some non-zero value (for quality of service purposes, for example). In this manner, when the TOS field is being used to specify a type of service request, it will only become ineffective in that regard *if* the source address cannot in fact be verified.

Moreover, in accordance with one illustrative embodiment of the present invention, packets coming from a peer carrier that also implements an embodiment of the present invention would be advantageously accepted without further checks. Packets from a non-participating peer carrier, however, would advantageously have the TOS field set to zero, since the originating source address could not be verified in such a case.

In accordance with the above-described illustrative embodiments of the present invention, one modest side effect resulting from the use of the instant technique may be to penalize packets that are or might be forged and yet want to have high quality-of-service. But, advantageously, no packets at all are dropped by the network, and therefore no existing applications will be broken, unlike, for example, the more stringent ingress filtering prior art approach described above (and in IETF RFC 2267).

Note that the most expensive part of implementing the above-described illustrative embodiment of the present invention is the RPF (or other) test of incoming

packets on access lines, but routers already exist that implement this efficiently. Note also that the implementation of an embodiment of the present invention is not incompatible with certain ones of the above-described prior art approaches, such as, for example, the use of IPsec, and indeed, use of the present invention may make it easier to defend IPsec tunnels against denial of service attacks.

Brief Description of the Drawings

Figure 1 shows an illustrative structure of a typical IP (Internet Protocol) data packet which may be routed with use of an IP CallerID service in accordance with an illustrative embodiment of the present invention.

Figure 2 shows an illustrative network environment comprising two carriers which offer an IP CallerID service in accordance with an illustrative embodiment of the present invention.

Figure 3 shows a flowchart of an illustrative method for processing an incoming packet to provide an IP CallerID service in accordance with an illustrative embodiment of the present invention.

Figure 4 shows a flowchart of an illustrative method for processing a packet received at a destination in accordance with an illustrative embodiment of the present invention, wherein the packet has been advantageously processed by a carrier providing an IP CallerID service in accordance with an illustrative embodiment of the present invention such as that of the illustrative method shown in Figure 3.

Detailed Description of the Illustrative Embodiments

Figure 1 shows an illustrative structure of a typical IP (Internet Protocol) data packet which may be routed with use of an IP CallerID service in accordance with an illustrative embodiment of the present invention. The illustrative IP data packet begins with an indication in data field 11 that the packet is an IPv4 (version 4) protocol data packet. Data field 12 comprises a Type-of-Service (TOS) value which may, in some illustrative embodiments of the present invention, be used by the sender to indicate quality of service information (*i.e.*, a desired or required quality of service level provided by the sender). In other illustrative embodiments of the present invention (*e.g.*, where quality of service information is not provided), the TOS field may simply be left blank by the sender.

Finally, in data field 13 of the illustrative IP data packet, the source address is specified. This address is supposed to identify the originating IP address of the packet. However, in certain situations, such as when the packet is generated maliciously from a denial of service attack which employs IP address spoofing, the source address indicated in data field 13 may, in fact, be erroneous ("spoofed").

Figure 2 shows an illustrative network environment comprising two carriers which offer an IP CallerID service in accordance with an illustrative embodiment of the present invention. The illustrative environment shown in the figure includes (malicious) "smurfer" 21 who, for example, is attempting to perpetrate a denial of service attack by sending IP packets with fake ("smurfed") source addresses into network 23 of carrier A. Specifically, these packets are received by edge (periphery)

router 23A of network 23. Network edge router 23A (as well as all of the other network edge routers shown in the figure) may be a Border Gateway Protocol (BGP) router, fully familiar to those of ordinary skill in the art.

Meanwhile, (legitimate) system 22 is sending legitimate IP packets having real (*i.e.,* correct) source addresses into network 24 of carrier B. Specifically, these packets are received by edge (periphery) router 24A of network 24. In addition, there is the possibility that IP packets arrive in general from (untrusted) Internet 25 and are received, for example, by edge (periphery) router 24C of network 24. (Edge routers 23B and 24B are also shown in the figure – they may be used for the exchange of IP packets between network 23 and network 24 as needed.)

In accordance with the illustrative embodiment of the present invention, carrier A and carrier B offer a "premium" IP CallerID service to (premium) customer 26. In particular, IP packets forwarded to customer 26 will have their TOS data field set to a non-zero value *if and only if* the source address identified in the packet has been "verified." As shown, "smurfed" IP packets sent, for example, by (malicious) smurfer 21, will be forwarded to customer 26 with their corresponding TOS fields set to a value of zero, while legitimate packets sent, for example, by (legitimate) system 22, will be forwarded to customer 26 with their corresponding TOS fields set to a non-zero value.

Note that in other illustrative embodiments of the present invention, data fields other than the TOS field may be used to provide an indication of whether the source address has been verified or not. For example, any otherwise unused field (of one or

more bits) in the IP data packet may be used as a "flag" which is set to zero or non-zero (*e.g.*, one) based on whether the source address has been verified or not.

Figure 3 shows a flowchart of an illustrative method for processing an incoming packet to provide an IP CallerID service in accordance with an illustrative embodiment of the present invention. The illustrative method of Figure 3 may be advantageously employed by a network edge (periphery) router in response to the network receiving an incoming IP packet.

Specifically, after an IP packet is received by the edge router (as shown in block 31 of the figure), an RPF (Reverse Path Forwarding) test or other similar such test is performed to verify whether the given IP packet has, in fact, come from the identified source address (as shown in block 32 of the figure). (Reverse Path Forwarding tests are conventional and fully familiar to those of ordinary skill in the art.) Decision 33 determines whether the RPF (or other) test has succeeded, and if not, block 36 sets the TOS field equal to a value of zero. If the source address does, in fact, pass the RPF (or other) test, decision 34 determines whether the TOS field has a zero value, and if so, block 35 sets the value of the TOS field equal to one. Finally, the packet is forwarded (block 37 of the figure) with the TOS field set to a non-zero or zero value based on whether the source address has been verified or not.

Note that if the TOS field is being used for quality of service purposes, then in accordance with this illustrative embodiment of the present invention, any non-zero TOS value provided by the sender will not be disturbed *as long as the source address can be verified.* In other words, only unverified IP packets will lose their indicia of

required or requested quality of service treatment. Also note that, as described above, in accordance with other illustrative embodiments of the present invention, a data field of the IP data packet *other than* the TOS field may be used to indicate whether the source address has been verified or not.

Figure 4 shows a flowchart of an illustrative method for processing a packet received at a destination in accordance with an illustrative embodiment of the present invention, wherein the packet has been advantageously processed by a carrier providing an IP CallerID service in accordance with an illustrative embodiment of the present invention such as that of the illustrative method shown in Figure 3. The packet is received by block 41 and decision 42 checks the value of the TOS field in the received packet. If the TOS field value is equal to zero, the packet is rejected and discarded (block 46) since the IP source address has not been verified.

If, on the other hand, the TOS field is not equal to zero, the (verified) source address is looked up in a table (block 43) which advantageously contains acceptable and/or unacceptable known addresses. Decision 44 then determines whether the source address is acceptable or unacceptable based on the lookup performed in block 43. If it is acceptable, the packet is accepted and forwarded (block 45). Otherwise, it is rejected and discarded (block 46).

Note that in accordance with certain illustrative embodiments of the present invention, the table lookup of the illustrative method shown in Figure 4 is not performed. Rather, the packet is accepted (and forwarded) or rejected (and discarded) based solely on whether the TOS field value is equal to zero or not equal to zero. And

in certain other illustrative embodiments of the present invention, all received packets are accepted (and forwarded), regardless of the value of the TOS field. However, in accordance with these embodiments, the data packets are advantageously prioritized based on whether the source address has been verified or not (*e.g.,* whether the TOS field value is equal to zero or not equal to zero). In this manner, no packets whatsoever are lost, but "smurfed" packets such as those sent as apart of a denial of service attack will be given lower priority and thus will be quite ineffective at interfering with the handling of legitimate data packets (which is the goal of a denial of service attack).

Addendum to the detailed description

It should be noted that all of the preceding discussion merely illustrates the general principles of the invention. It will be appreciated that those skilled in the art will be able to devise various other arrangements, which, although not explicitly described or shown herein, embody the principles of the invention, and are included within its spirit and scope. In addition, all examples and conditional language recited herein are principally intended expressly to be only for pedagogical purposes to aid the reader in understanding the principles of the invention and the concepts contributed by the inventor to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions. Moreover, all statements herein reciting principles, aspects, and embodiments of the invention, as well as specific examples thereof, are intended to encompass both structural and

functional equivalents thereof. It is also intended that such equivalents include both currently known equivalents as well as equivalents developed in the future – *i.e.,* any elements developed that perform the same function, regardless of structure.